FRC 2016
9ème édition

LA GENDARMERIE D'ALSACE
& LES OFFICIERS DE LA RÉSERVE CITOYENNE

AD HONORES
Réseau ALSACE

9ème FORUM DU RHIN SUPÉRIEUR SUR LES CYBERMENACES

LA CYBERCRIMINALITÉ : UN BUSINESS LUCRATIF

www.frc.alsace

@cybermenaces

9ÈME FORUM DU RHIN SUPÉRIEUR SUR LES CYBERMENACES

2009

2010

2011

2012

2013

2014

2015

2016

NOTRE OBJECTIF

"Mobiliser les décideurs des PME-PMI d'Alsace afin que ceux-ci mettent en œuvre les actions nécessaires à leur entreprise, face aux risques liés aux technologies du numériques".

- **Animation : Gilbert GOZLAN**

  Directeur Opérationnel Sûreté Réseau La Poste Nord & Est

  Lieutenant-Colonel (RC) de la Gendarmerie Nationale

  Président de l'association AD HONORES Réseau Alsace

9ÈME FORUM DU RHIN SUPÉRIEUR SUR LES CYBERMENACES

Discours d'ouverture

- **Général Stéphane OTTAVI**

  Commandant adjoint de la région de gendarmerie
  Alsace-Champagne-Ardenne-Lorraine
  Commandant le groupement de gendarmerie départementale du Bas-Rhin

9ÈME FORUM DU RHIN SUPÉRIEUR SUR LES CYBERMENACES

Discours d'ouverture

- **Bernard STIRNWEISS**

  Président de la CCI de la région Alsace

9ÈME FORUM DU RHIN SUPÉRIEUR SUR LES CYBERMENACES

Discours d'ouverture

- **François SCHRICKE**

  Ingénieur principal territorial, chargé du Pôle « politiques publiques » à la préfecture de la région Grand Est, préfecture du Bas Rhin

9ème FORUM DU RHIN SUPÉRIEUR SUR LES CYBERMENACES

Salle de conférence de l'ENA

PROGRAMME FRC 2016 9ème édition

13h00 — ACCUEIL

13h30 — DISCOURS D'OUVERTURE

Général Stéphane OTTAVI
Commandant adjoint de la région de gendarmerie Grand Est.
Commandant le groupement de gendarmerie départementale du Bas-Rhin.

Bernard STIRNWEISS
Président de la CCI Alsace.

■ Animation
Gilbert GOZLAN
Directeur Sûreté du Réseau la Poste Nord & Est.
Lieutenant Colonel (RC) de la gendarmerie nationale.
Président de l'association AD HONORES Réseau Alsace.

14h00 — CONFERENCE D'OUVERTURE

PANORAMA DES MOYENS JURIDIQUES DE LUTTE ACTUELS ET ATTENDUS CONTRE LES CYBERMENACES

Myriam QUEMENER
Magistrat - Docteur en droit - Conseiller Juridique du Préfet en charge de la lutte contre les Cybermenaces, conseiller du gouvernement.

14h30 — TABLE RONDE #1

LA CYBERCRIMINALITE : UN BUSINESS LUCRATIF

Colonel Philippe BAUDOIN
Chargé de mission, Cabinet du Directeur Général de la gendarmerie nationale, coordinateur pour les Cybermenaces.

Régis PIERRE
Vice-Président chargé de l'instruction, juridiction interrégionale spécialisée, TGI de Nancy.

Adjudant Jean Claude LE BUHE
Section de Recherches de la gendarmerie de Strasbourg.
Division délinquance économique, financière et numérique.

Jean-François THONY
Procureur Général près la cour d'appel de Colmar, ancien directeur de l'école nationale de la magistrature.

15h40 — PAUSE / DÉTENTE

16h20 — TABLE RONDE #2

... POURTANT DES SOLUTIONS EXISTENT

Julien GAMBA / Nicolas RENARD / Vinh LUONG
Etudiants en Master 2 Réseaux informatiques et systèmes embarqués.

Benjamin CHETIOUI
Etudiant en Master 2 Ingénierie du logiciel et des connaissances.
Université de Strasbourg.

Ludovic HAYE
Consultant chez DBI Services. Chef d'escadron (RC) de la gendarmerie nationale.

Daniel GUINIER
Expert près la cour pénale internationale de la Haye.
Colonel (RC) de la gendarmerie nationale.

Laurent SCHMERBER
Président 3MA Group. Chef d'escadron (RC) de la gendarmerie nationale.

17h40 — CONFERENCE DE CLÔTURE

Général d'armée (2S) Marc WATIN AUGOUARD
Ancien inspecteur des armées-gendarmerie. Directeur du Centre de Recherche de l'Ecole des Officiers de la Gendarmerie Nationale (CREOGN).

18h30 — COCKTAIL DE FIN DE FORUM

www.frc.alsace

@cybermenaces

LA CYBERCRIMINALITÉ UN BUSINESS LUCRATIF.

NOS SPONSORS

NOS SPONSORS

CCI ALSACE

NOS SPONSORS

NOS SPONSORS

NOS SPONSORS

NOS SPONSORS

NOS SPONSORS

NOS SPONSORS

NOS SPONSORS

NOS SPONSORS

NOS SPONSORS

NOS SPONSORS

LA CYBERCRIMINALITÉ
UN BUSINESS LUCRATIF

Panorama des moyens et techniques de l'investigation numérique

- **Daniel GUINIER**

  Expert en cybercriminalité et crimes financiers près la Cour pénale internationale de La Haye

  Expert de justice honoraire près la cour d'appel de Colmar

  Colonel (RC) de la gendarmerie nationale

Introduction et cadre juridique

FORMES D'ACTIVITES CRIMINELLES « CYBER »

- **Les formes traditionnelles de criminalité – *favorisées***
  - *ex. délinquance astucieuse, faux et usage de faux, extraction de données*
- **La diffusion de contenus illicites par voie électronique**
  - *ex. pornographie enfantine, atteinte à la propriété intellectuelle*
- **Les infractions propres aux réseaux électroniques**
  - *ex. attaques visant les systèmes d'information, usurpation d'identité*

Tous en lien avec la convention de Budapest sur la cybercriminalité du Conseil de l'Europe du 23/11/01 (STCE n°185)

Le territoire est mondial et les actes instantanés, tandis que les législations sont hétérogènes et la coopération internationale encore difficile.

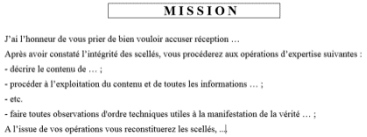
CADRE JURIDIQUE ET ETAPES

En matière pénale - Procédure correctionnelle ou procédure criminelle
Enquête : sur **réquisition** par OPJ : préliminaire : Art. 77-1 ; de flagrance : Art. 60 du CPP
Instruction : sur **ordonnance** du magistrat instructeur - Arts.156 et suivants du CPP

Tribunal correctionnel, C Assises, CA
Citation à comparaître ; Arts. 437, 438 du CPP ; remise par huissier de justice

Listes par spécialité
Expert unique ou dualité d'experts

1. Désignation et mission de l'expert


MISSION

J'ai l'honneur de vous prier de bien vouloir accuser réception …
Après avoir constaté l'intégrité des scellés, vous procéderez aux opérations d'expertise suivantes :
- décrire le contenu de … ;
- procéder à l'exploitation du contenu et de toutes les informations … ;
- etc.
- faire toutes observations d'ordre techniques utiles à la manifestation de la vérité … ;
A l'issue de vos opérations vous reconstituerez les scellés, …

Urgence : sans délai, sinon
Art. 161-1 du CPP : 10 jours

Début de mission
Remise des scellés
Devis éventuel
Ouverture scellés
Investigations

Rapport et conclusion
Dépôt du rapport
Reconstitution et restitution des scellés
Fin de la mission

2. Opérations d'expertise

Prestation de serment
Déposition
Questionnement

3. Procès : *Cour d'Assises ou autre*

Expert judiciaire inscrit ou prêtant serment avant le début de mission

Liste d'une CA
Liste nationale de la CC

Expert honoraire
Spécialiste reconnu

Expert-témoin prêtant serment

En matière civile - Mesures d'instruction en référé ou sur requête, exécutées, notamment sur les fondements de l'Art.145 du CPC.
L'ordonnance désigne les acteurs et précise le champ de la mission et les opérations autorisées, sous contrôle d'un huissier de justice.

Etape 0 : Le dépôt de plainte permet le début de l'action judiciaire.

CONTEXTE DE LA PREUVE

- **Aspects juridiques**
  - Légalité - *respect de la loi et des procédures*
  - Pertinence - *en rapport avec les faits*
  - Authenticité - *nature, origine, création*
  - Admissibilité - *copie à la place de l'original*
  - Véracité - *intégrité du contenu*

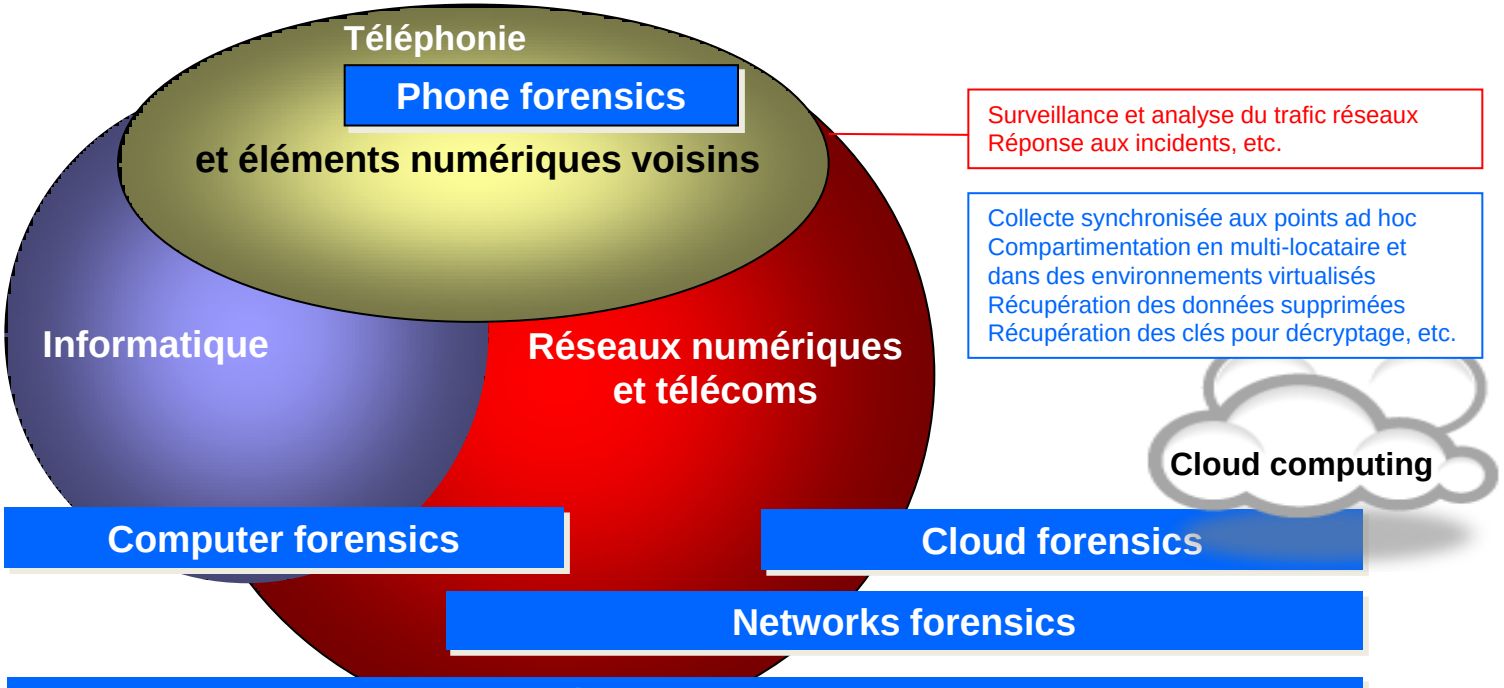
- **Aspects méthodiques et techniques**
  - Accessibilité - *locale ou distante*
  - Fiabilité - *collecte et représentation*
  - Authentification - *auteurs et horodatage des actes*
  - Conservation - *support et transfert*
  - Présentation - *pédagogie adaptée*

Contexte de l'investigation numérique

Les traces électroniques sont fugaces, la recherche de preuves débute souvent des semaines, voire des mois après les faits, et le signalement comme les saisies sont parfois tardives, d'où l'importance d'une réaction rapide.

L'INFORENSIQUE

L'inforensique est **une discipline** portant sur les **connaissances**, **méthodes** et **outils** ayant pour **objectifs** la collecte ou l'extraction, la conservation et l'analyse de données numériques, et pour **finalité** la garantie de présentation des résultats en tant que **preuves légales recevables**.



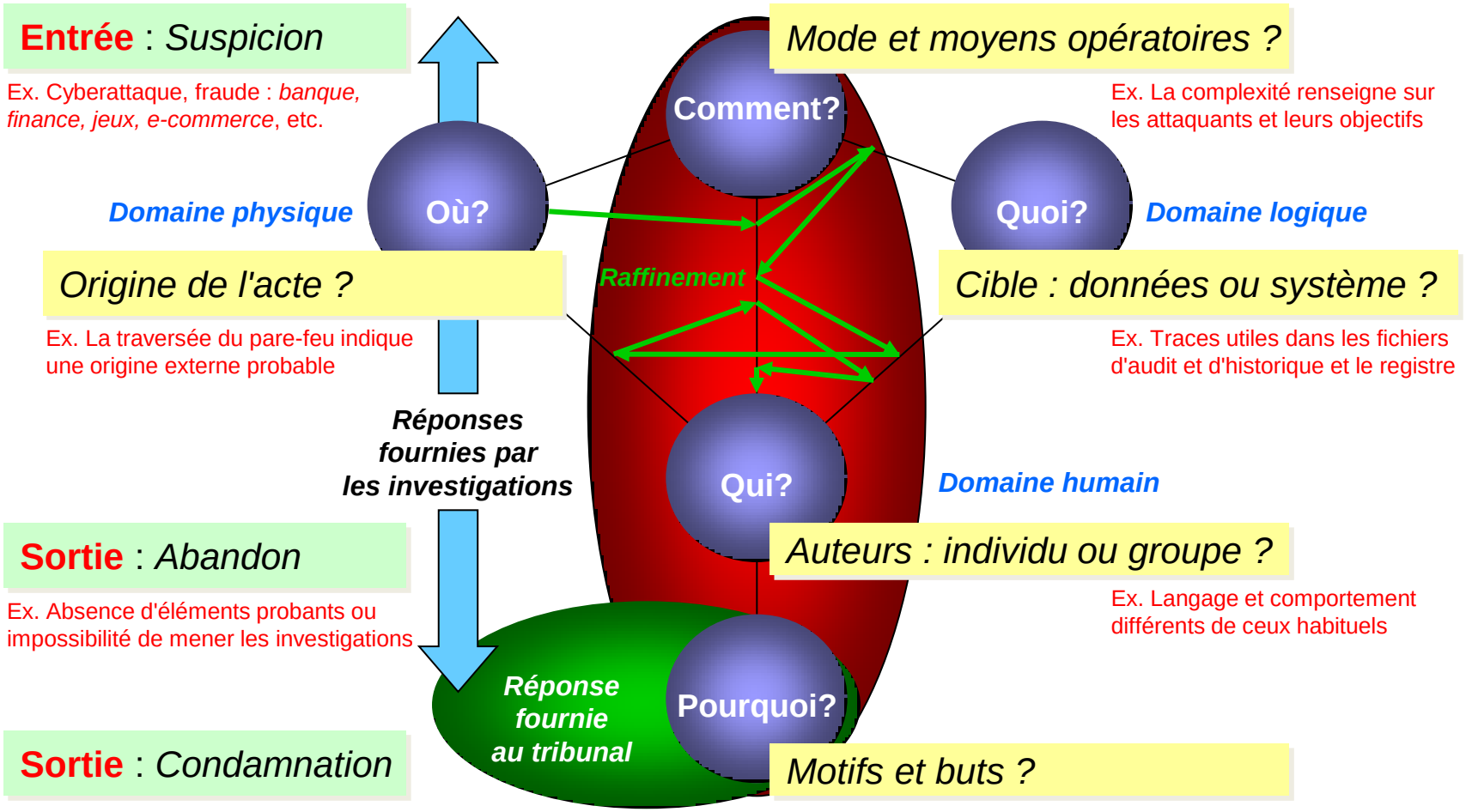
L'inforensique représente une partie importante du processus d'investigation, intégré aux chaînes d'enquête et de criminalistique.

CYCLE DE L'INVESTIGATION NUMERIQUE

- **La collecte et la préservation**
  - *ex. collecte des données, très volatiles et autres, protection des supports*
- **L'exploitation des éléments collectés**
  - *ex. extraction des données, analyses, compléments au niveau physique*
- **La présentation des preuves**
  - *ex. rapport, conclusion, réponses aux questions, déposition sous serment*

Il est nécessaire de remonter à la source parfois plusieurs mois après les faits, y compris dans un contexte international et multi-juridictionnel.

QUESTIONS RELEVANT DES INVESTIGATIONS



Les indices sérieux et concordants viennent s'ajouter à mesure des avancées pour répondre aux questions essentielles.

LA SCENE DE CRIME NUMERIQUE

Connexions

Points d'accès

INVESTIGATIONS EN COURS

Mémoire RAM

Equipements réseaux
Organes de raccordement

DVD
CD

Bandes

Objets connectés ou non

Cartes mémoire

Clés USB

Disques externes

SSD

Serveurs internes

SCENE DE CRIME A PRESERVER

Imprimantes photocopieurs

Poubelle …

Consoles de jeu

SCENE DE CRIME A PRESERVER

Cartes SIM

Cartes mémoire

Microordinateurs portables, unités centrales et accessoires

Tablettes, téléphones, GPS appareils photo, caméras, baladeurs

Serveurs externes

Virtualisation dans des méga-centres

"Cloud"

Multi-territorialité
Légitimité
Souveraineté

Où ? A l'étranger …

INVESTIGATIONS EN COURS

Coopération internationale

Transmissions

LES INDICES NUMERIQUES

Côté victime

Postes de travail et périphériques
Connexions et organes de communications

Côté serveurs

Applications
Données, NAS
Sauvegarde
Messagerie
Téléphonie IP
Web, etc.

4

5

Interconnexion

Commutateurs	(OSI 2) MAC
Routeurs	(OSI 3) IP
Pare-feux	(OSI 3-4)
Proxies	(OSI 5-7)

Côté "cloud"

Côté suspect

Postes de travail et périphériques
Connexions et organes de communications

Côté FSI

6

FSI : Fournisseur de Services Internet

Principe de Locard : ***"Nul ne peut agir sans laisser des marques multiples de son passage"***

(Dr. Edmond Locard (1877-1966))

GEL ET PREALABLES EN VUE DES ANALYSES

Microordinateurs portables, unités centrales et serveurs

Analyse directe : *"Live forensics"*

En fonctionnement : *bruit, activité, etc.*
Ne pas couper l'alimentation électrique

Appeler un spécialiste compétent habilité pour :
Obtention de **données volatiles** : caches, processus, fichiers temporaires et d'échanges *(ex. Pagefile.sys)*, fichier de veille prolongée *(hiberfile.sys), etc.*
Capture du contenu de la **mémoire vive (RAM)** pour analyse et obtention de clés et de mots de passe, etc.

Si indisponibilité ou après capture de ces éléments :
Mettre hors fonctionnement
en coupant l'alimentation électrique

En cas de crypto-attaque, il est attendu d'isoler les machines par leur déconnexion au plus vite *(ex. **cas de rançongiciel**)*

Analyse différée : *'Post mortem"*

Hors fonctionnement
Ne pas mettre en fonctionnement

Marquer l'ensemble des connexions et leurs câbles
Retirer l'ensemble des cordons d'alimentation
Photographier et documenter l'ensemble
Emballer de façon à protéger et à assurer le transport
Mettre sous scellé dans le cadre de la procédure, pour **expertise** avec des moyens inforensiques

Connexions : Microordinateurs portables, unités centrales et serveurs, organes de raccordement et d'interconnexion

Débridage ? ***PIN ?***

Code clavier ?

Horodatage ?

Téléphones et tablettes

Analyse directe : *"Live forensics"*

En fonctionnement : *écran, home, etc.*
Ne pas éteindre, mais éviter toute connexion : *réseaux télécoms ou autre*

Appeler un spécialiste compétent habilité pour :
Préserver l'intégrité et éviter l'écriture / reset à distance
Supprimer l'extinction temporisée, *tout en le notant*
Réaliser l'analyse au mieux, noter l'horodatage indiqué

Si indisponibilité ou après ces éléments :
Mettre hors fonctionnement
en état d'arrêt total

Nombre de téléphones ne sont pas exploitables sans le code de déverrouillage du clavier.

Analyse différée : *"Post mortem"*

Hors fonctionnement
Ne pas mettre en fonctionnement

Documenter : Marque, modèle, noter le **débridage**, le **code PIN** carte SIM **et de déverrouillage du clavier**
Faire en sorte d'éviter tout démarrage inopiné
Emballer de façon à protéger et à assurer le transport
Mettre sous scellé dans le cadre de la procédure, pour **expertise** avec des moyens inforensiques

L'investigation numérique concernant l'informatique et les éléments voisins

LES METHODES ET OUTILS INFORENSIQUES

- **Les méthodes**
  - de copie
    - au niveau logique : *répertoires et fichiers existants*
    - au niveau physique : *réplique du disque bit-à-bit (clone)*
  - d'investigation ; *protégée par un dispositif de blocage*
    - analyse au niveau logique, *y compris éléments supprimés*
    - analyse au niveau physique, *à l'aide de mots-clés*
- **Les outils**
  - de copie
    - par un matériel inforensique performant *(Tableau TD2)*
    - par un logiciel ou suite logicielle inforensique
  - d'investigation ; *par une suite logicielle inforensique éprouvée*
    - au niveau logique, relativement aux traces enregistrées ou supprimées
    - au niveau physique, relativement aux traces rémanentes

RECHERCHE AVANCEE PAR « Data Carving »

- **Extraction et restitution de fichiers effacés**

Image partielle restante

Image présentant 3 parties superposées

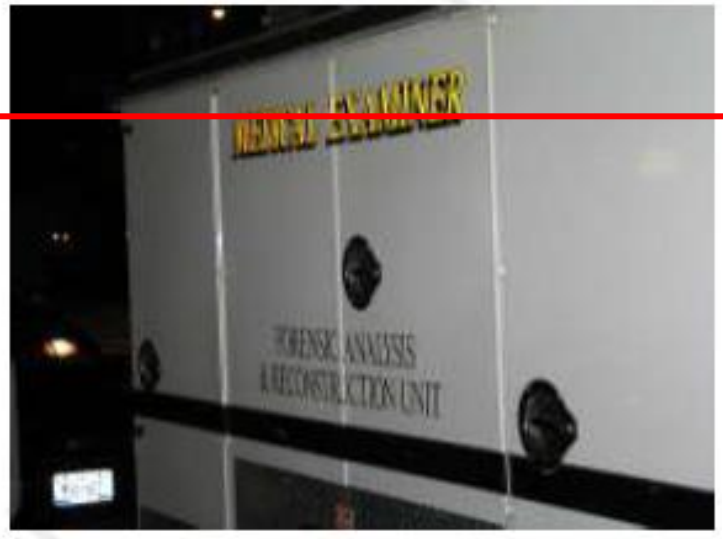


Image complète initiale

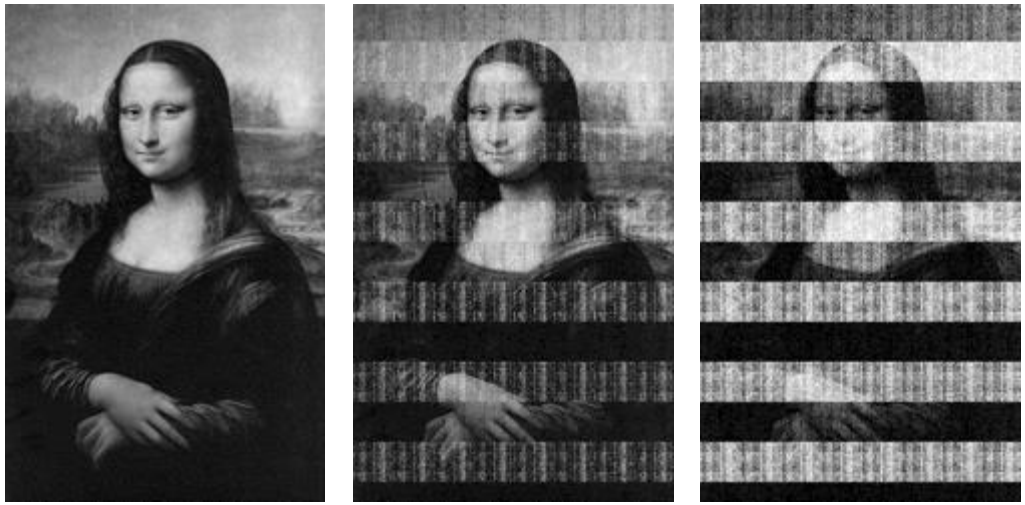
Il est possible de retrouver des fichiers effacés, de façon partielle ou totale, par la recherche de l'entête *("header")* et du bas de page *("footer")* typiques de chaque type *(ex. Start-of-image (SOI) : FF D8, et FF D9 pour .jpg)*.

VOLATILITE DE LA MÉMOIRE VIVE

- **Volatilité *versus* rémanence de la mémoire vive RAM**

après 30 s

après 1 mn



J. A. Haldermann et al.(2009) : *Lest we remember : Cold-boot attacks on encryption keys, Comm. ACM, vol. 52, n° 5, mai 2009, pp. 91-99*

Fragments volatiles en RAM

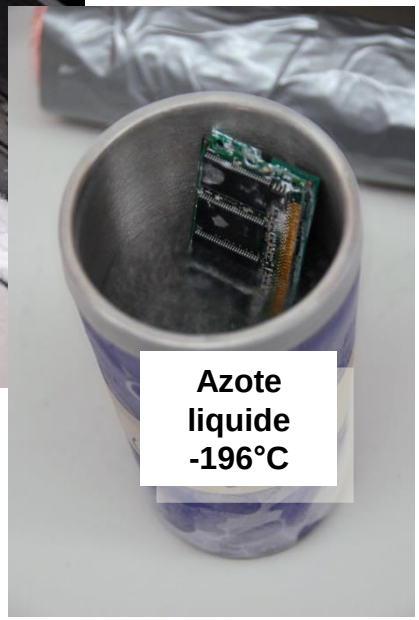
Sessions, services et processus en cours
et utilisateurs et périphériques connectés
Parties de **code malveillant en RAM**
Clés cryptographiques et mots de passe
Informations : *registre, système, démarrage, documents, images, etc*., qui n'ont **pas encore été sauvegardés sur disque** (Ports ouverts et à l'écoute, caches : *ARP, DNS, ...*),
etc.

ARP (Protocole de résolution d'adresse)
traduit une **adresse logique** (ex. **IP**) de réseau (OSI 3) en une **adresse physique MAC** (Media Access Control) de liaison (OSI 2)
DNS (Système de noms de domaines)
traduit un **nom de domaine** en informations diverses, notamment en **adresse IP** de la machine portant ce nom.

Il serait possible de retrouver des informations utiles après une minute, à la température ambiante, par le recours à une méthode de correction d'erreurs.

CONSERVATION DE LA MÉMOIRE VIVE

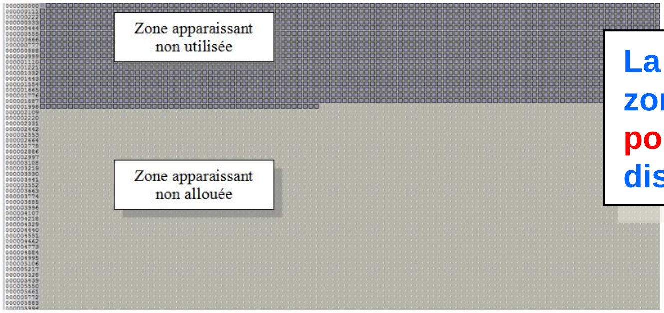
- ***"Gel"* en l'état des données fixées par cryogénie**



J. A. Haldermann et al.(2009) : Lest we remember : Cold-boot attacks on encryption keys, Comm. ACM, vol. 52, n° 5, mai 2009, pp. 91-99

Ceci permettrait la recherche de clés, lorsque l'accès *"cold-boot"* est verrouillé et d'accéder au système. Une copie sera faite à l'aide d'un logiciel *"RAM imager"* *(FTK, EnCase, Belkasoft, Dumpit, Passware, etc.).*

QUAND LE DISQUE DUR EST CRYPTE…



La surface du disque apparaît alors divisée en 2 zones : *non utilisée et non allouée*, comme suit, **pouvant laisser penser à tort qu'il s'agit d'un disque non formaté dépourvu de partition**

Ces traces sont ici présentées **codées ASCII sous la forme d'un texte** :

```
ê·|··  TrueCrypt  Boot  Loader   ·ú3ÀŽØŽÐ¼·|ûö·¶}·u·□6·|èÜ·¸·□□>··h·}·¸€□>··(·}·¸·  ŽÀ2À¿··¹ÿžüóªŒÀ-
··ŽÀ±·º·»··è´·f3Û¾··¹··èº·fS»·          ±·º9ö·F}·t·º·±$è‘·f[¾·          ‹·º}è—·f;·²}t%ö·F}·u·Æ·F          }·±
ö··}·u-□6U}èS·□6·|èL·ëþŒÀŽØúŽÐ¼·€ûRh                                        h·zh·□·hç|·h··ËƒÄ·Z··…Àt
      □6U}è··ëþŠ6·}ŒÀ···ŽÀŽØúŽÐ¼üŸû·h··Ë3Û´·ü¬,Àt·Í·ë÷Ãµ·¶·´·Í·s·□6G}èàÿÃ···f3Àü¬f·ØfÑÃâ÷·Ã·Disk
error ···Loader  damaged! Use Rescue Disk: Repair Options > Restore·························ò.¾è····È·-ñ·€
!··þÿÿ·····¬·············································U ª
```

ou **codées en Hexadécimal** :

```
EA 1E 7C 00 00 20 54 72 75 65 43 72 79 70 74 20 42 6F 6F 74 20 4C 6F 61 64 65 72 0D 0A 00 FA 33 C0 8E D8 8E
D0 BC 00 7C FB F6 06 B6 7D 01 75 07 8D 36 05 7C E8 DC 00 B8 00 90 81 3E 13 04 68 02 7D 0E B8 00 80 81 3E
13 04 28 02 7D 03 B8 00 20 8E C0 32 C0 BF 00 01 B9 FF 9E FC F3 AA 8C C0 2D 00 08 8E C0 B1 02 B0 04 BB 00
01 E8 B4 00 66 33 DB BE 00 01 B9 00 08 E8 BA 00 66 53 BB 00 0D B1 06 B0 39 F6 06 46 7D 01 74 04 B0 1A B1
24 E8 91 00 66 5B BE 00 0D 8B 0E B0 7D E8 97 00 66 3B 1E B2 7D 74 25 F6 06 46 7D 01 75 0E C6 06 46 7D 01
B1 20 F6 06 B7 7D 02 75 AD 8D 36 55 7D E8 53 00 8D 36 05 7C E8 4C 00 EB FE 8C C0 8E D8 FA 8E D0 BC 00 80
FB 52 68 0A 0D 68 00 7A 68 00 81 0E 68 E7 7C 06 68 00 01 CB 83 C4 06 5A 0E 1F 85 C0 74 09 8D 36 55 7D E8 1B
00 EB FE 8A 36 B7 7D 8C C0 05 00 08 8E C0 8E D8 FA 8E D0 BC FC 9F FB 06 68 00 01 CB 33 DB B4 0E FC AC
84 C0 74 04 CD 10 EB F7 C3 B5 00 B6 00 B4 02 CD 13 73 07 8D 36 47 7D E8 E0 FF C3 1E 06 1F 66 33 C0 FC AC
66 03 D8 66 D1 C3 E2 F7 1F C3 00 44 69 73 6B 20 65 72 72 6F 72 0D 0A 07 00 07 4C 6F 61 64 65 72 20 64 61 6D
61 67 65 64 21 20 55 73 65 20 52 65 73 63 75 65 20 44 69 73 6B 3A 20 52 65 70 61 69 72 20 4F 70 74 69 6F 6E 73
20 3E 20 52 65 73 74 6F 72 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 07 1A F2 2E BE E8 1C 08 00 06 C8 0F 2D F1 00 00 80 20 21 00 07 FE FF FF 00 08 00 00 00 18 AC 0E 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA
```

La confirmation est produite par le progiciel Passware Kit Forensic, *de Passware Inc. (USA)*, qui indique la protection suivante sur le disque SSD :

Protection: **TrueCrypt System Volume - Open Password**

Complexity: **Brute-force - Slow, Hardware acceleration possible**

L'investigation numérique concernant les téléphones et les éléments voisins

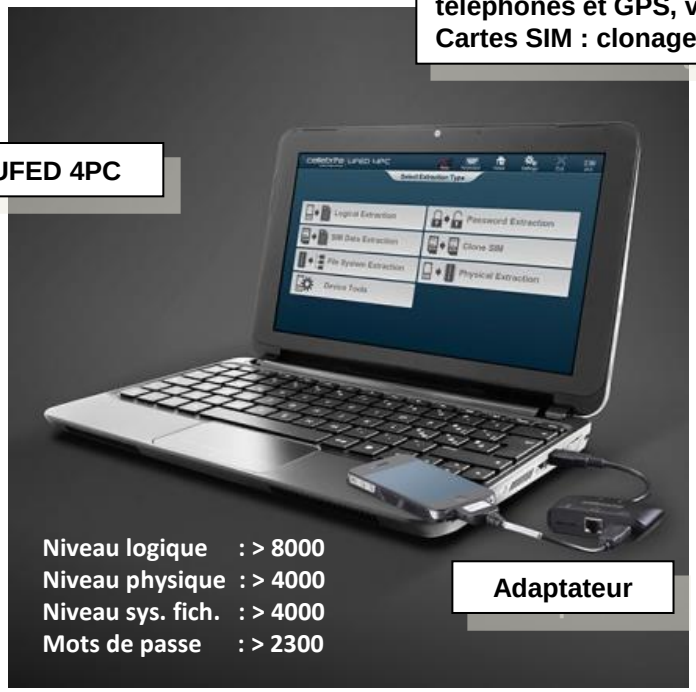
Smartphones
Tablettes
Systèmes GPS

PLATEFORME D'EXTRACTION ET D'ANALYSE

- **Solution logicielle *versus* solution matérielle** *(ex. Cellebrite Inc.)*

L'extraction sur près de 20 000 modèles de téléphones et GPS, via USB, RJ 45 et Bluetooth
Cartes SIM : clonage des identifiants et extraction

UFED 4PC



UFED Classic

UFED Touch

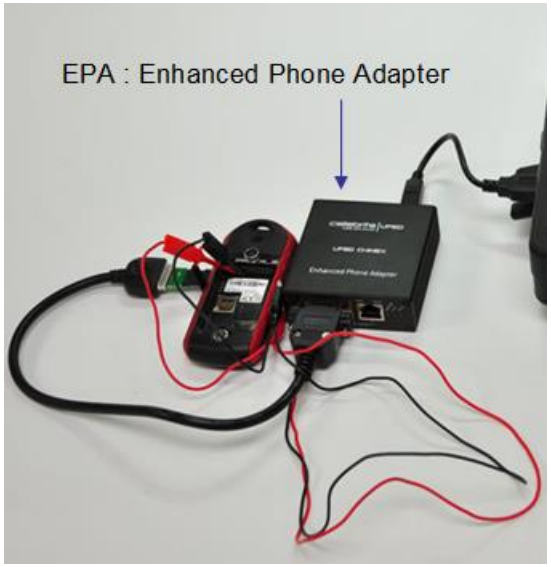
La solution UFED 4PC apparaît souple et performante en fonction du PC pour l'extraction comme pour l'analyse. Elle nécessite souvent l'adaptateur ad hoc.

EXTRACTION DES COMBNES « CHINOIS »

Kit CHINEX

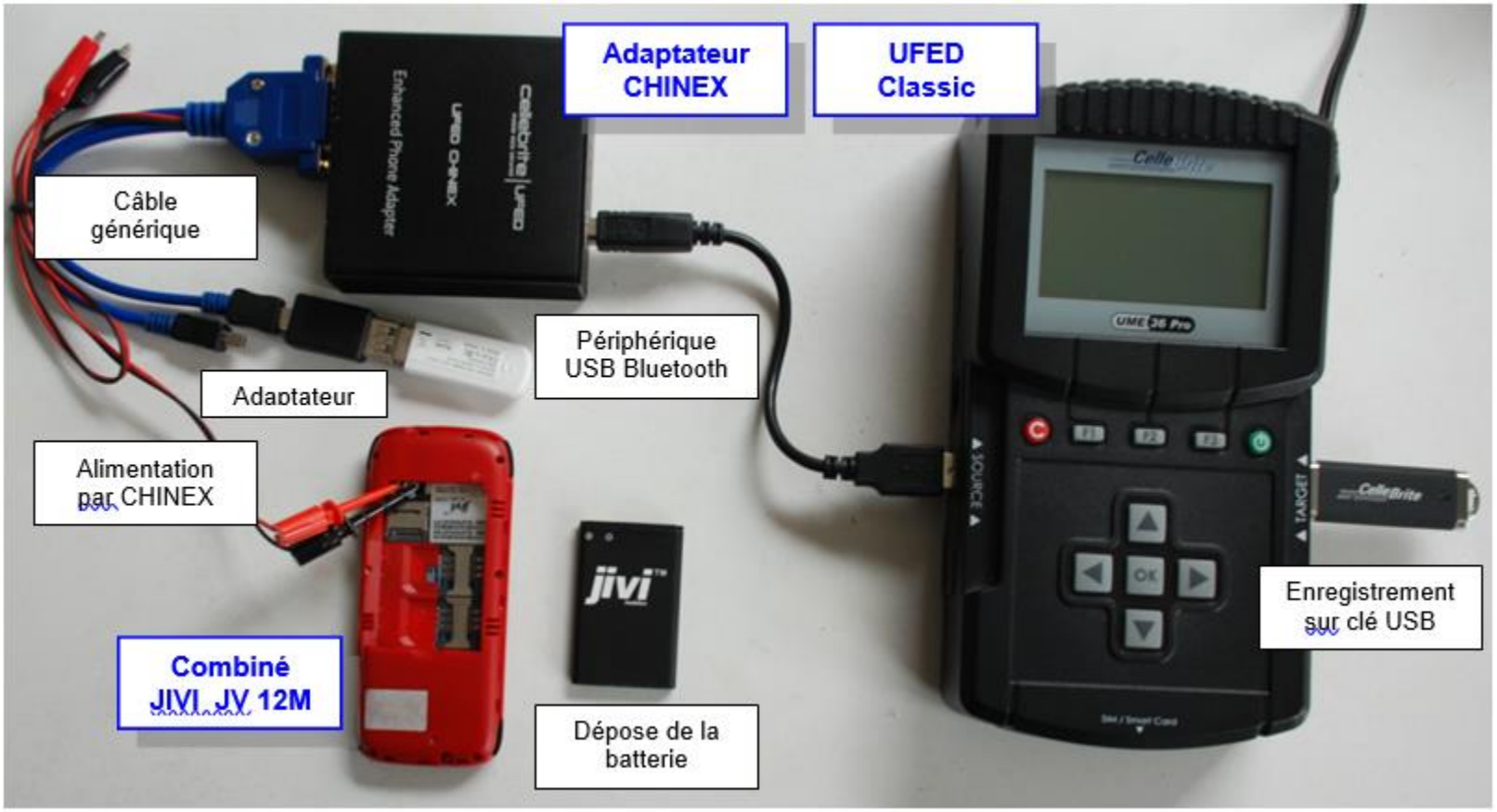
- EPA
- Câbles
- Connecteurs

Marché : MTK (Mediatek), Spreadtrum, Infineon



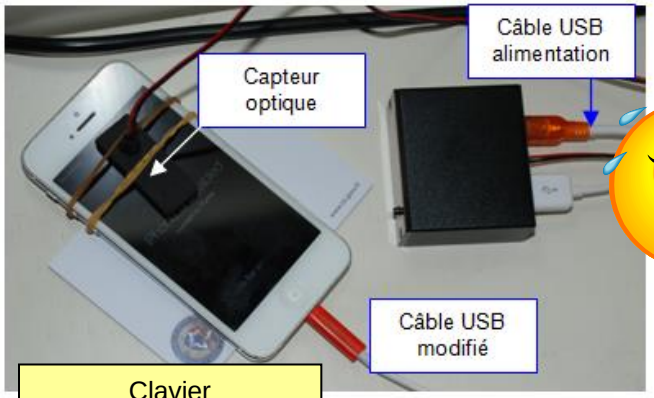
Connexion avec UFED
Classic, Touch ou 4PC

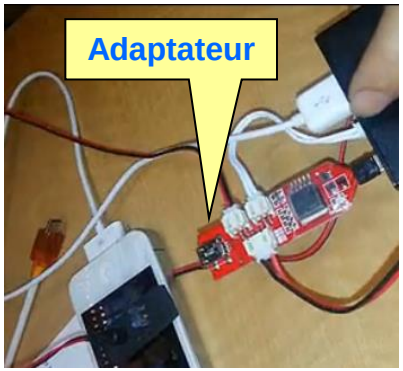
EXTRACTION COMPLEXE MIXTE



Recours à une connexion Bluetooth si le combiné ne dispose pas de port USB.

QUAND LE CLAVIER EST VERROUILLE…





… et que toute analyse est impossible : Première réalisée en 2014 avec un iPhone 5. Des opérations plus complexe après l'iOS 8.1.0, et une impossibilité d'agir avec les versions iOS 9 et suivantes, dès 2015 quelques mois après !

Capture distante

Capture par aspiration de site Web
Capture par interception de données

CAPTURE PAR INTERCEPTION DE DONNEES

(Loi portant adaptation de la procédure pénale au droit de l'UE, vu la convention de Budapest sur la cybercriminalité du CE du 23/11/01).

- **Cadre juridique**
  - **Loi n° 2015-993** du 17 août 2015 - Art. 11(1)
  - **Infractions** prévues aux Arts. 706-73 et 706-73-1 relevant de crime organisé
  - **Décision et contrôle** du juge d'instruction
  - **Art. 706-102-2 du CPP** : il est précisé la localisation ou la description des STAD
  - **Décret n° 2018-1700** du 18 décembre 2015 sur les modalités de mise en œuvre de la captation en application de l'**Art. 706-102-1 du CPP**

- **Moyen et objectifs**
  - Mise en place d'un **dispositif technique** avec pour objectifs, sans consentement des intéressés, d'**accéder**, en tous lieux, à des données informatiques, de les **enregistrer**, les **conserver** et les **transmettre**, telles qu'elles s'affichent sur un écran de l'utilisateur d'un STAD, ou qu'elles sont introduites ou reçues et émises par des périphériques audiovisuels.

(STAD : Système de Traitement Automatisé de Données)

- **Conditions**
  - **Connaissance et accessibilité de la cible** : informatique ou téléphone
  - **Injection** à distance d'un cheval de Troie ad hoc, possible par la messagerie
  - **Capacité d'exploiter l**es données transmises
  - **Désactivation ou suppression** après un délai de 4 mois, ou prolongation.

Ce cadre relève de l'interception plutôt que de la e-perquisition, du fait des moyens de transmission des données capturées.

CONCLUSION

- **La preuve numérique nécessite**
  - la coopération : public-privé et judiciaire au plan international
  - la collecte, préservation, analyse et présentation des indices
  - le recours à des méthodes et outils adéquats
  - la mutualisation des moyens inforensiques coûteux
- **L'inforensique nécessite à son tour**
  - des experts certifiés de haut niveau typiquement *"pénalistes"*
  - un savoir-faire, des compétences et une formation adaptée
  - une remise à niveau constante, différente des experts *"civilistes"*
  - la maîtrise à jour des technologies et de leurs imperfections

L'expertise inforensique se fonde sur la recherche et le partage des savoirs, mais aussi par la curiosité et l'expérimentation, pour satisfaire la confiance, et souvent même le doute utile …

DIFFICULTES TECHNIQUES ET PERSPECTIVE

- **Le cryptage des données**
  - profite à la cybercriminalité et au crime organisé
  - freine ou empêche les investigations numériques
- **Les acteurs comme Apple et d'autres**
  - en font un gage de sécurité sans discernement
  - refusent d'offrir des moyens de décryptage aux autorités
- **Les solutions multi-parties de décryptage envisageables**
  - **un tiers de confiance** qui authentifie les entités et assure la sécurité
  - **trois entités garantes** :
    - le **garant du système judiciaire** (ex. l'autorité chargée de l'instruction)
    - le **garant du système technique** : *fabriquant ou opérateur* (ex. Apple)
    - le **garant des libertés formellement reconnu**(ex. la CNIL)
  - **l'entité d'investigation** (ex. l'enquêteur désigné)

Guinier D. (1995) : CLIPSoft ® : Systèmes garants multi-parties destinés à la surveillance légale des télécommunications. Dépôt n° 41837 à l'INPI, Paris.

FRC 2016 : LA CYBERCRIMINALITÉ UN BUSINESS LUCRATIF

TABLES RONDES

- La cybercriminalité : un business lucratif
- ….. Pourtant des solutions existent

TABLE RONDE 1

La cybercriminalité : un business lucratif

LA CYBERCRIMINALITÉ : UN BUSINESS LUCRATIF

- **Colonel Philippe BAUDOIN**
  Chargé de mission - Coordinateur pour les cybermenaces
  Cabinet du Directeur Général de la Gendarmerie Nationale
- **Régis PIERRE**
  Vice-président chargé d'instruction
  Juridiction Interrégionale Spécialisée – TGI de Nancy
- **Adjudant chef Jean-Claude LE BUHE**
  Section de Recherche de la Gendarmerie de Strasbourg
  Division délinquance économique, financière et numérique
- **Jean-François THONY**
  Procureur Général près la cour d'Appel de Colmar
  Ancien directeur de l'école nationale de la magistrature

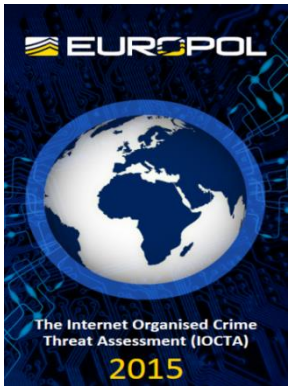
LA CYBERCRIMINALITÉ : UN BUSINESS LUCRATIF

Montée des menaces pour le tissu économique et industriel français malwares et ingénierie sociale

Colonel Philippe BAUDOIN

TENDANCES

- **Les chiffres de la cybercriminalité ?**
  - Pas de statistiques officielles (hors STAD)
  - Continuum entre la criminalité classique et celle liée aux technologies numériques
  - Centre de lutte contre les criminalités numériques : 80 % escroqueries, 10 % atteintes aux systèmes informatiques
  - Nécessité de signaler les incidents aux autorités (GN, PN, DGSI, ANSSI)
- **Typologie des cibles et tendances**
  - Administrations / PME-PMI & ETI / Grandes entreprises
  - Modes opératoires : exploitation de vulnérabilités sur serveurs, mails piégés
  - i-OCTA Europol : Cybercrime as a service
  - Haut niveau de cybermenaces :
  - montée des extorsions et des fraudes



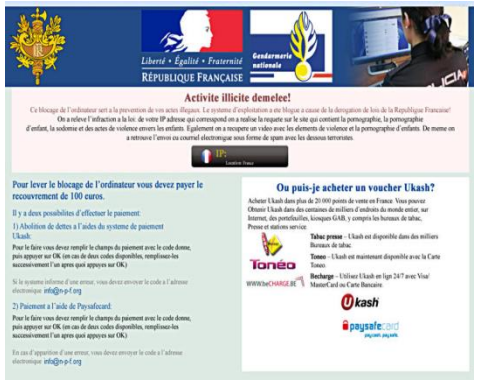
VOL DE DONNEES BANCAIRES

- **Chevaux de Troie – virus bancaire Dridex**
  - Pièce jointe infectée dans un mail
  - Fuite des données de connexion au compte bancaire en ligne
  - Réalisation de virements frauduleux vers des mules
  - Expansion rapide – préjudice important

- **Situation actualisée**
  - Arrestation d'un administrateur fin 2015 à Chypre et saisie de serveurs de commande par FBI et EC3. Mais persistance du phénomène
  - Solution : anti-virus et antispyware à jour
  - Après une montée en puissance du phénomène au cours de 2015, le nombre d'infection apparaît aujourd'hui en régression
  - Illustration de l'impact possible d'un virus sur l’économie

RANCONGICIELS

- **Historique**
  - 2011 ransomware bloquant les systèmes d'exploitation et exigeant une « amende ». Fin 2013 apparition de cryptovirus
  - Modes opératoires
  - Incriminations: extorsion de fonds sous contrainte / atteintes aux STAD
- **Evolution récente : Locky, Petya**
  - Chiffrement des postes compromis mais aussi des partages de fichiers
  - Ciblage orienté vers les sociétés et les entreprises
  - Rançon en bitcoin, d'incidence variable
  - Véritable menace sur tissu économique & industriel



- **Investigations et données utiles**
  - Audition victime, recueil du vecteur d'inoculation
  - Analyse du malware – Rôle d'Europol (EC3)
  - Compétence concurrente Parquet Paris – Traçabilité mail & Bitcoins

RANCONGICIELS

- **Préconisations**
  - Ne pas céder à la tentation de payer
  - Réinstallation totale du système d'exploration
  - Contacts possibles avec les éditeurs d'outils de sécurité
  - Signaler impérativement

- **Se prémunir contre les cryptovirus**
  - Mise à jour antivirus et antispyware
  - Utilisation d'un logiciel pour repérer les sites Internet sûrs,
  - d'une solution de sécurité pour repérer les fichiers infectés dans les mails
  - Ne pas cliquer dans les mails dont la provenance est inconnue
  - Sauvegarde régulière des données sur support non connecté

- **Sites d'information**

ANSSI : fiche de sensibilisation www.cert.ssi.gouv.fr/site/CERTFR-2016-ALE-001

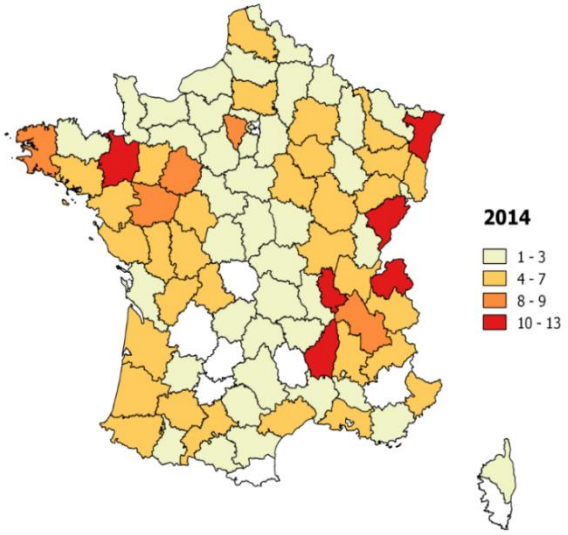
www.nomoreransom.org - No more ransomware - Europol

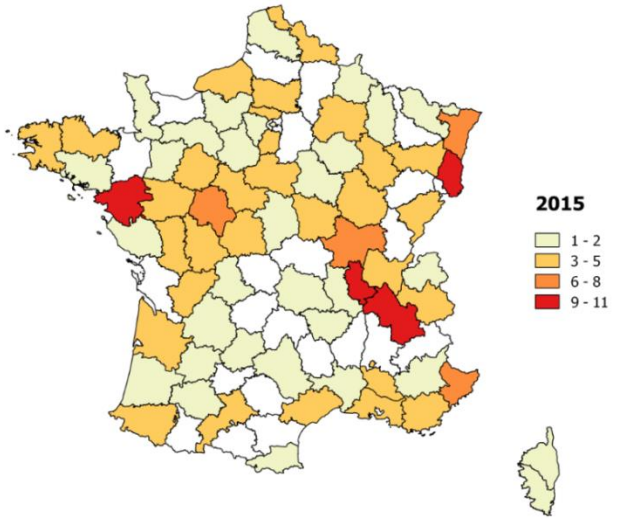
www.barracuda.com

FAUX ORDRES DE VIREMENT

- **Escroqueries FOVI : pillage organisé du patrimoine**
  - Phénomène : Recours à des moyens frauduleux (usage d'un faux nom ou d'une fausse qualité, une mise en scène) basés sur de l'ingénierie sociale
  - Utilisation de différents vecteurs et outils numériques
  - Plus de 250 millions d'euros sur les trois dernières années

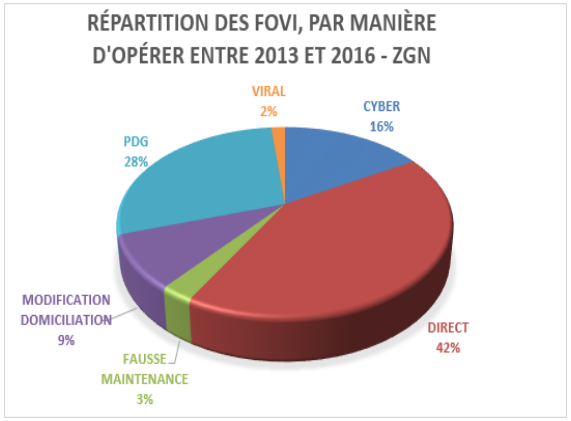
- **Etude & Analyse - *SCRC***
  - Géographie criminelle : sociétés victimes localisées dans des zones économiques à forte activité ou dans des zones frontalières

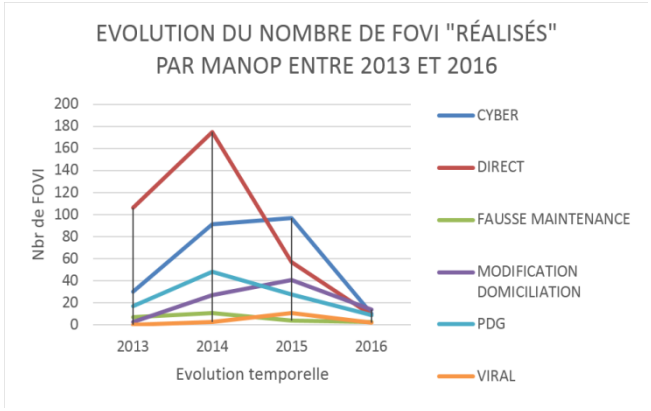




FAUX ORDRES DE VIVREMENT

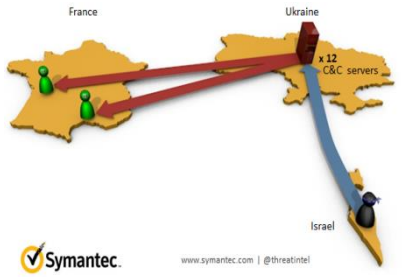
- **Etude & Analyse - *SCRC* (suite)**
  - Modes opératoires utilisés selon une stratégie à trois étages : étude préalable, passage à l'acte, récupération des fonds
    - Déclinaison récurrente selon six scenarii





    - Pics d'escroqueries aux mois de : mars, juillet, novembre et décembre
    - Pays destinataires : Chine et Pologne puis Royaume-Uni et Bulgarie

- **Investigations**
  - P.J., enquêteurs spécialisés, Renseignement
  - Tracfin, ARO, ASI, entraide pénale
  - Prévention : sensibiliser entreprises & banques



CONCLUSION

- **Darknets ?**
  - investigations possibles mais plus complexes

- **Enjeux**
  - Faire de la cybersécurité un process
  - Mise à jour des systèmes d'exploitation, applications et produits, patcher les failles (veiller)
  - Protéger les données (chiffrement et sauvegarde)
  - Formation de l'ensemble du personnel
  - Penser en globalité : cyber mais aussi accès physiques

LA CYBERCRIMINALITÉ : UN BUSINESS LUCRATIF

Intervention de l'autorité judiciaire et blocage du produit de l'escroquerie

Régis PIERRE

INTERVENTION DE L'AUTORITÉ JUDICIAIRE ET BLOCAGE DU PRODUIT DE L'ESCROQUERIE

1) Blocage extrajudiciaire du compte destinataire, et première investigations dans le cadre de la coopération pénale internationale

2) Gel du compte dans le cadre de l'enquête ou de l'information judiciaire

3) Confiscation finale des sommes saisies par la juridiction de jugement

INTERVENTION DE L'AUTORITÉ JUDICIAIRE ET BLOCAGE DU PRODUIT DE L'ESCROQUERIE

Introduction :

Les faux ordres de virements internationaux (FOVI)

- Principaux modes opératoires
- Le traitement judiciaire : l'action des JIRS

INTERVENTION DE L'AUTORITÉ JUDICIAIRE ET BLOCAGE DU PRODUIT DE L'ESCROQUERIE

1. Blocage extra judiciaire du compte et premières mesures judiciaires

- Blocage extra judiciaire
- Premières investigations dans le cadre de la coopération pénale internationale

INTERVENTION DE L'AUTORITÉ JUDICIAIRE ET BLOCAGE DU PRODUIT DE L'ESCROQUERIE

2. Gel judiciaire du produit de l'escroquerie

- Pays requis non membre de l'Union Européenne : la demande d'entraide pénale internationale classique aux fins de saisie du produit de l'escroquerie
- Pays requis membre de l'Union Européenne : une procédure simplifiée et accélérée : le certificat de gel

INTERVENTION DE L'AUTORITÉ JUDICIAIRE ET BLOCAGE DU PRODUIT DE L'ESCROQUERIE

3. La confiscation finale du produit du crime

- Pays requis non membre de l'Union Européenne
- Pays requis membre de l'Union Européenne

LA CYBERCRIMINALITÉ : UN BUSINESS LUCRATIF

Bilan d'une enquête internationale et des aspects financiers

Adjudant chef Jean-Claude LE BUHE

BILAN D'UNE ENQUÊTE INTERNATIONALE ET DES ASPECTS FINANCIERS

1) Typologie des infractions rencontrées :

- escroquerie en bande organisée, fait prévu et réprimé par les articles 313-1, 313-2313-7 et 313-8 du code pénal (natinf 7882),
- blanchiment aggravé, fait prévu et réprimé par les articles 324 et 132-71 du code pénal (natinf 27155),
- participation à une association de malfaiteurs, fait prévu et réprimé par les articles 450-1, 450-3 et 450-5 du code pénal (natinf 12214),
- usurpation de nom, de titre ou de qualité, fait prévu par les articles 433-18 et 433-22 du code pénal (natinf 108).
- accès ou maintien frauduleux dans un système de traitement automatisé de données, prévus et réprimés par les articles 323-1 et 323-5 du code pénal (natinf 1619 et 1637).

BILAN D'UNE ENQUÊTE INTERNATIONALE ET DES ASPECTS FINANCIERS

2) Investigations menées en France mais aussi et surtout à l'étranger :

En France :

- auditions des victimes et témoins, recueil d'un dépôt de plainte,
- recherche des éléments matériels (téléphonie, internet, éventuelle saisie du matériel pour analyse),
- interceptions téléphoniques, perquisition à distance,
- rapprochements judiciaires sur le territoire national.

A l'étranger :

- identification des sociétés et comptes bancaire à l'étranger, rapprochements judiciaires,
- suivi des flux financiers, identification des bénéficiaires économiques, localisation des retraits en espèces,
- localisation des mis en cause